E4-0026-TH(1)

(12) UK Patent Application (19) GB (11) 2 306 865 (13) A

(43) Date of A Publication 07.05.1997

(21) Application No 9621161.0

(22) Date of Filing 10.10.1996

(30) Priority Data
(31) 07271578 (32) 19.10.1995 (33) JP

(71) Applicant(s)
Fujitsu Limited

(Incorporated in Japan)

1015 Kamikodanaka, Nakahara-ku, Kawasaki-shi, Kanagawa 211, Japan

(72) Inventor(s)
Yasutsugu Kuroda

(74) Agent and/or Address for Service
Haseltine Lake & Co
Imperial House, 15-19 Kingsway, LONDON, WC2B 6UD, United Kingdom

(51) INT CL^6
H04L 9/32

(52) UK CL (Edition O)
H4P PDCSA

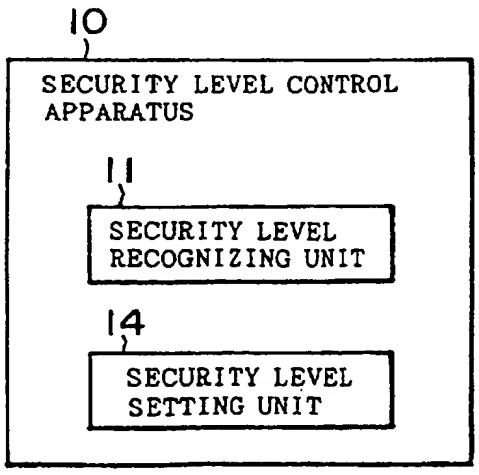
(56) Documents Cited
EP 0534679 A2 EP 0520709 A2 EP 0409397 A2
EP 0375139 A2 EP 0375138 A2 US 5369707 A

(58) Field of Search
UK CL (Edition O) H4P PDCSA PDCSX
INT CL^6 H04L 9/00 9/32
ONLINE : WPI

(54) Security level control apparatus and network communication system

(57) A security level control apparatus (10) for controlling the security level of communication between communication parties, comprises a security level recognizing unit (11) which recognizes a security level notified from a communication party and sets the security level for the security level control apparatus. As a result, communication can be established between the communication parties without presetting the security level. In one embodiment, security level control apparatuses at server and client network stations set a security level for communication from levels notified by the server and client. Communication takes place using encryption and session key exchange.

FIG. 1



GB 2 306 865 A

FIG. 1

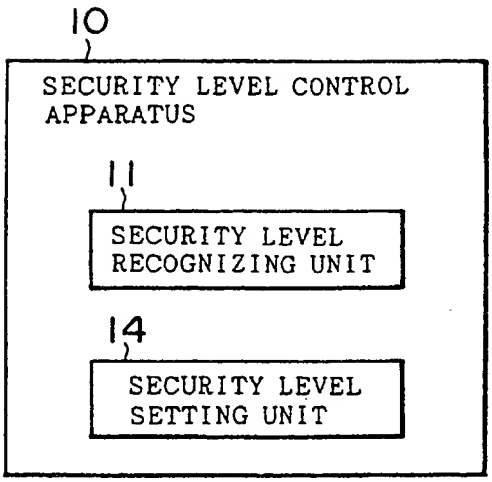


FIG. 2

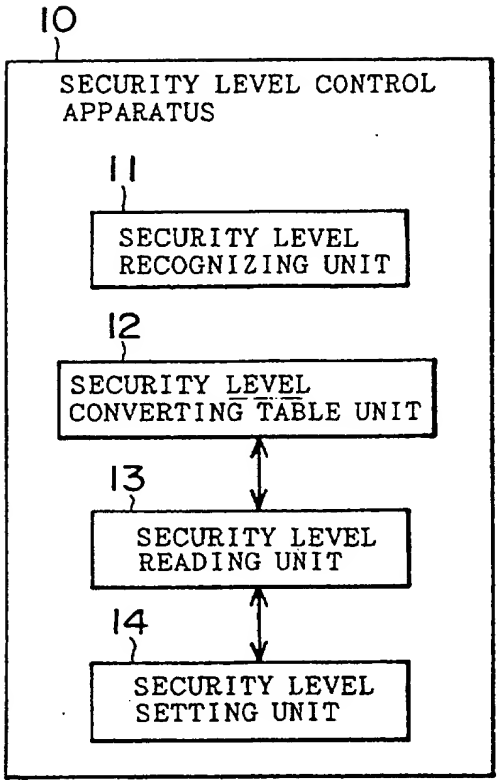

10
SECURITY LEVEL CONTROL APPARATUS
11
SECURITY LEVEL RECOGNIZING UNIT
12
SECURITY LEVEL CONVERTING TABLE UNIT
13
SECURITY LEVEL READING UNIT
14
SECURITY LEVEL SETTING UNIT

FIG. 3

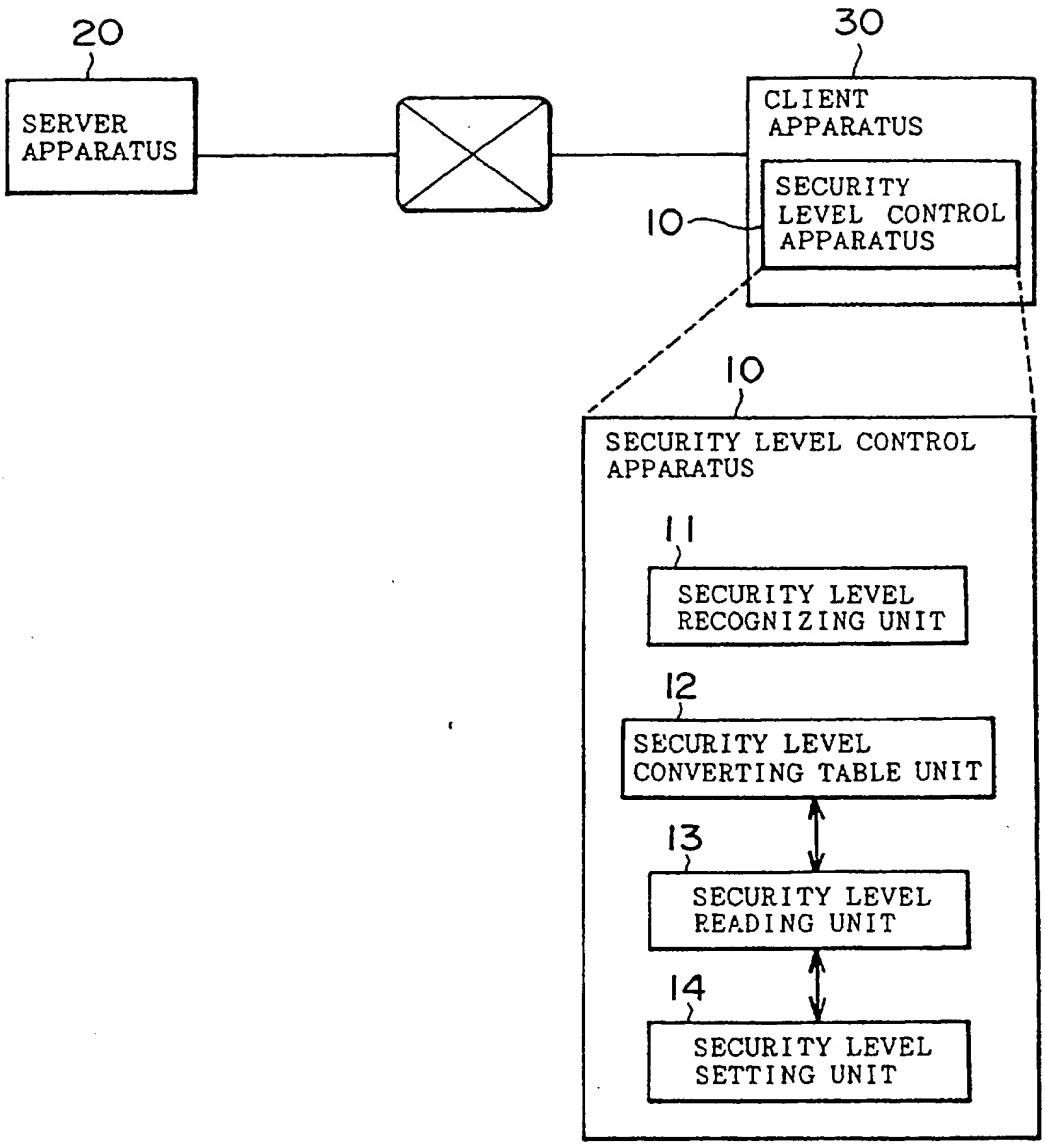


FIG. 4

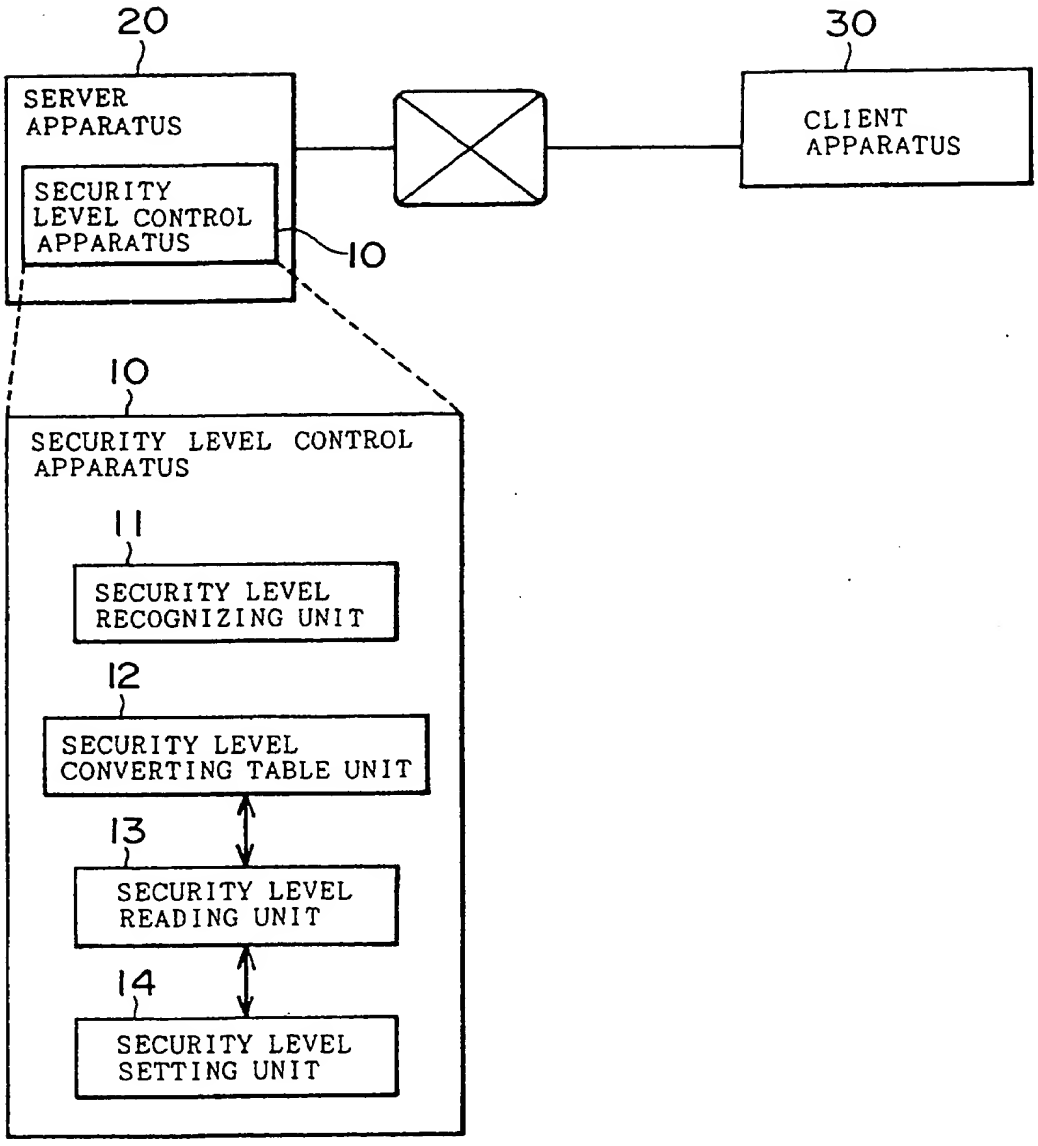

20
SERVER APPARATUS
SECURITY LEVEL CONTROL APPARATUS
10
30
CLIENT APPARATUS
10
SECURITY LEVEL CONTROL APPARATUS
11
SECURITY LEVEL RECOGNIZING UNIT
12
SECURITY LEVEL CONVERTING TABLE UNIT
13
SECURITY LEVEL READING UNIT
14
SECURITY LEVEL SETTING UNIT

FIG. 5

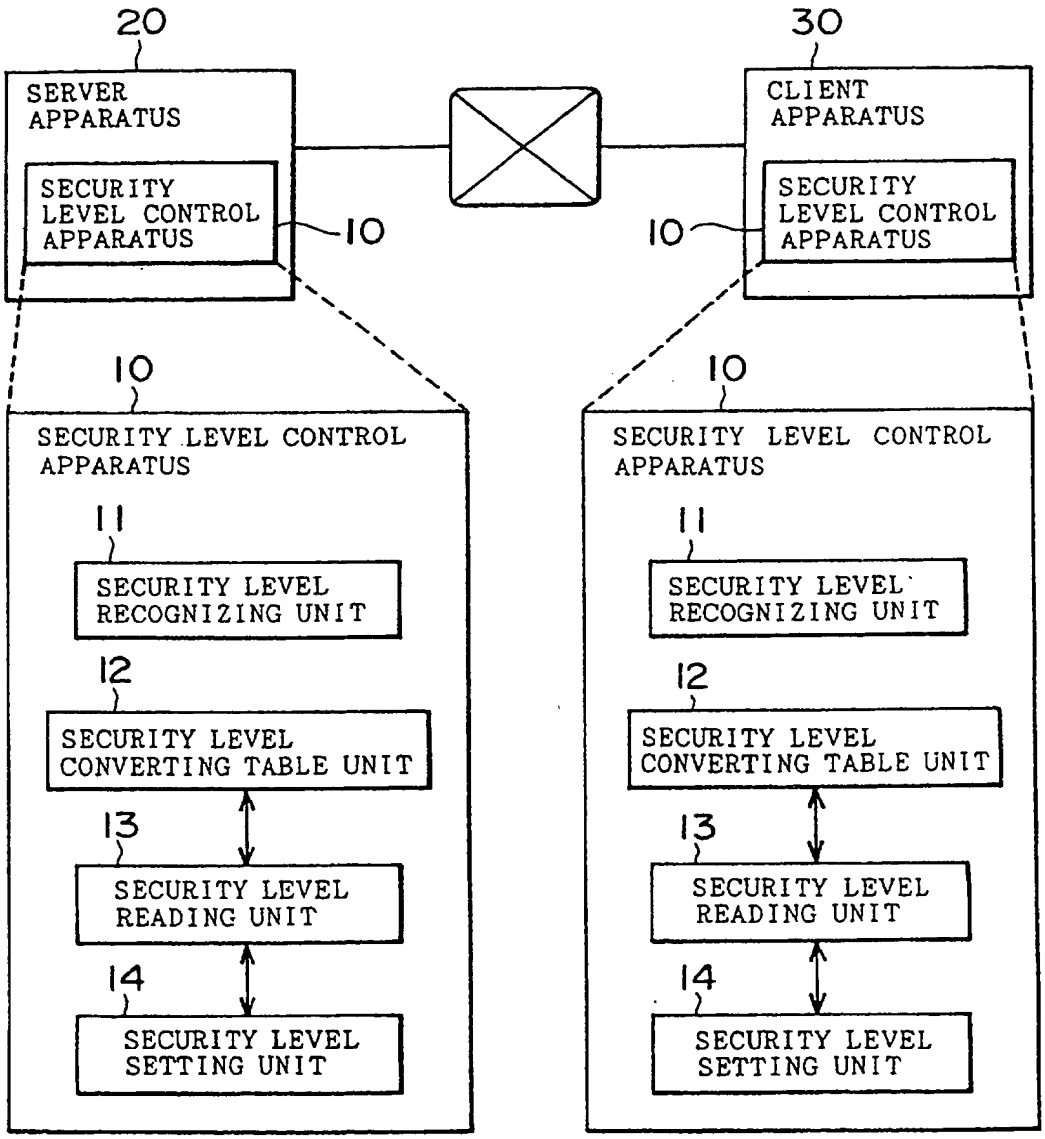


FIG. 6

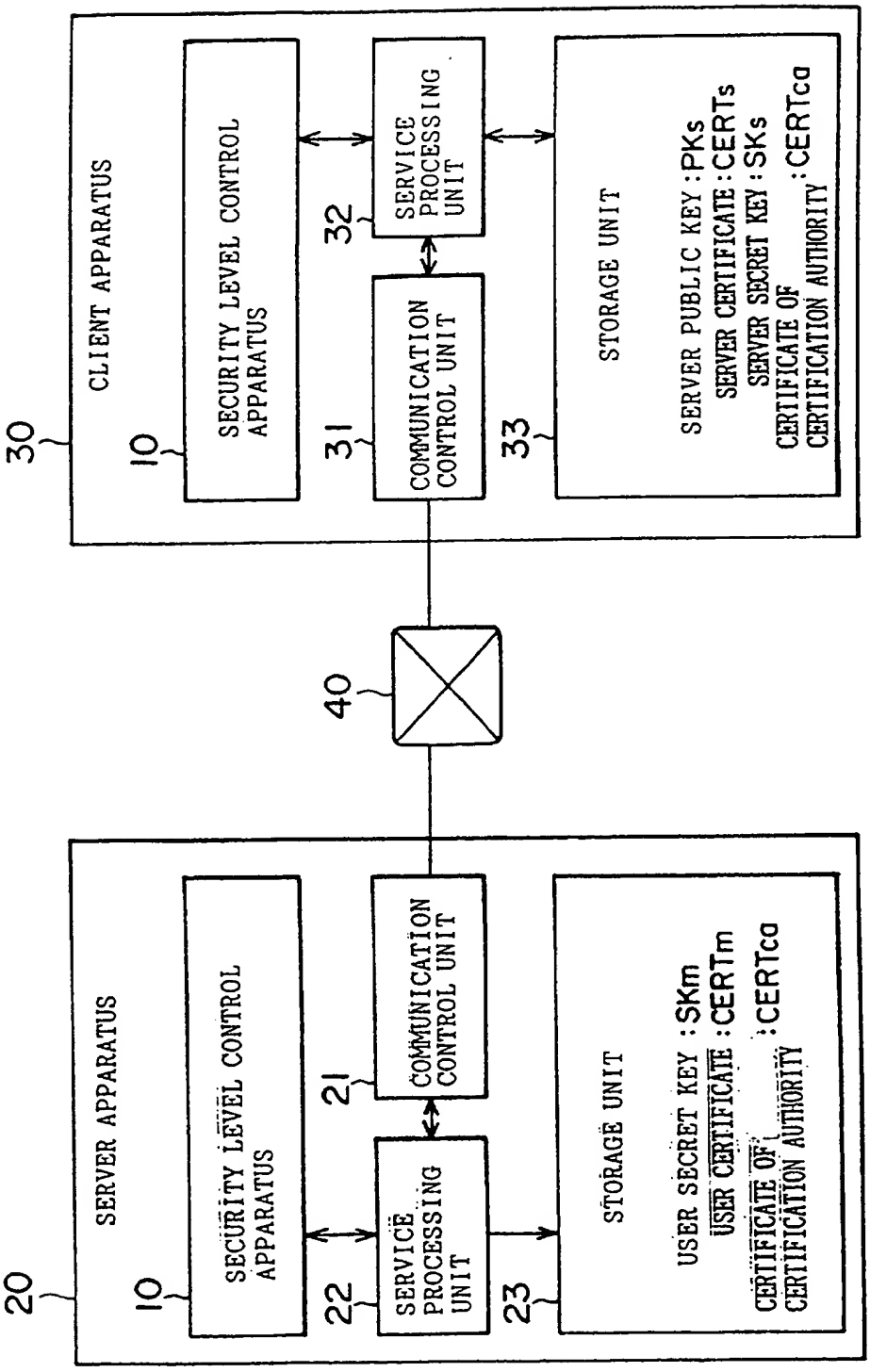


FIG. 7

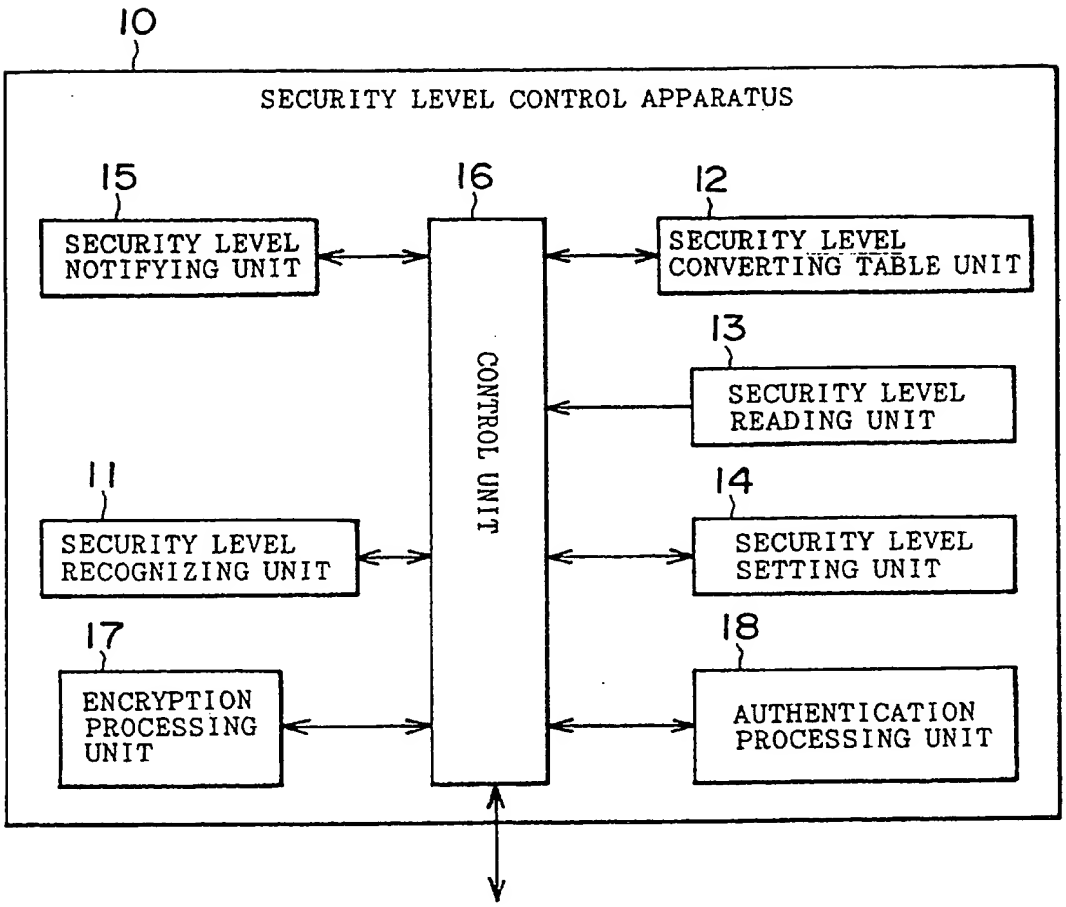

10
SECURITY LEVEL CONTROL APPARATUS
15
SECURITY LEVEL NOTIFYING UNIT
16
CONTROL UNIT
12
SECURITY LEVEL CONVERTING TABLE UNIT
13
SECURITY LEVEL READING UNIT
11
SECURITY LEVEL RECOGNIZING UNIT
14
SECURITY LEVEL SETTING UNIT
17
ENCRYPTION PROCESSING UNIT
18
AUTHENTICATION PROCESSING UNIT

FIG. 8

SECURITY LEVEL OF CLIENT \ SECURITY LEVEL OF SERVER	1	2	3	4	5
1	1	2	×	4	×
2	2	2	×	4	×
3	×	2	3	×	5
4	×	×	×	4	×
5	×	×	×	4	5

FIG. 9

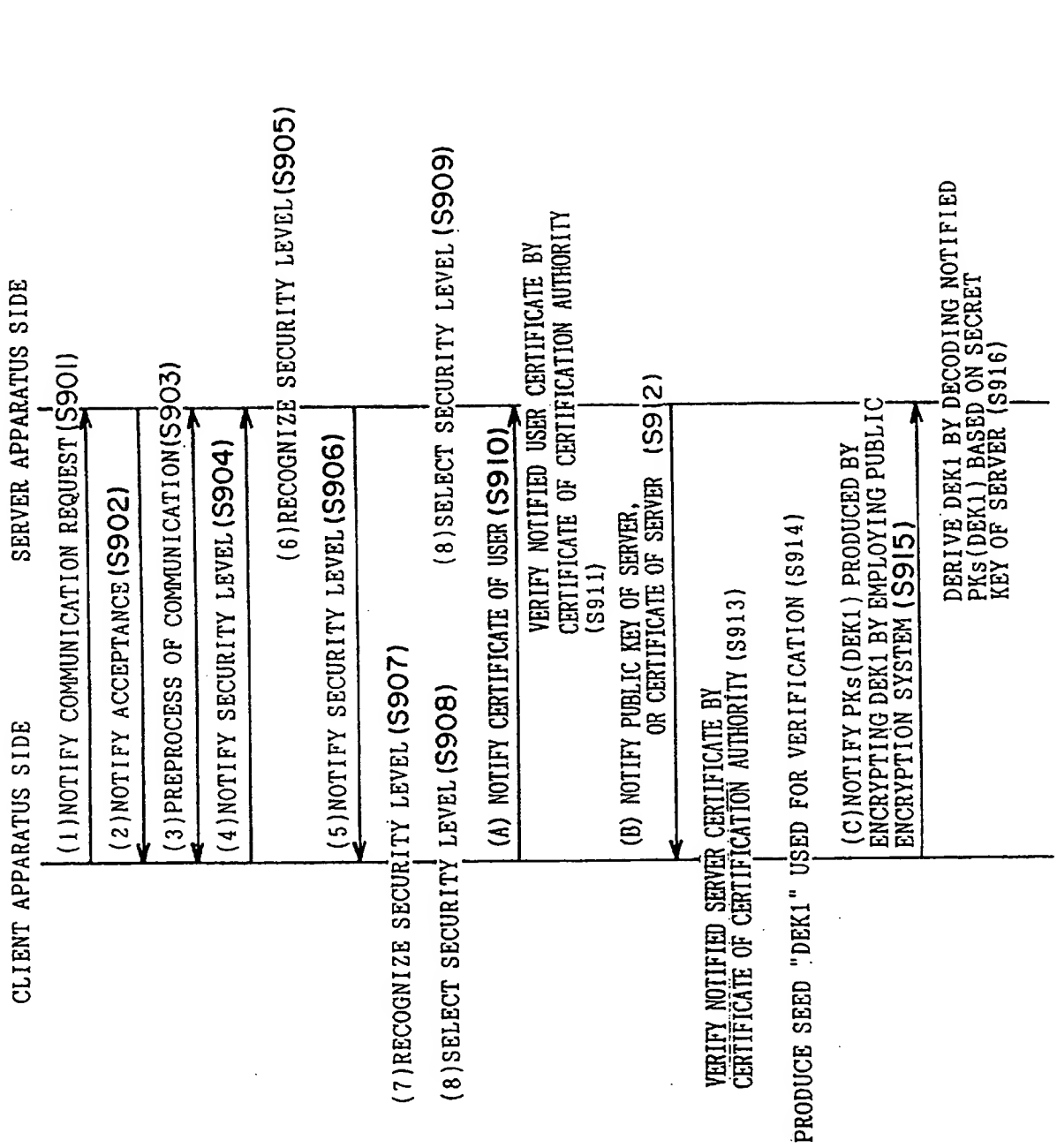

CLIENT APPARATUS SIDE
SERVER APPARATUS SIDE
(1)NOTIFY COMMUNICATION REQUEST (S901)
(2)NOTIFY ACCEPTANCE (S902)
(3)PREPROCESS OF COMMUNICATION (S903)
(4)NOTIFY SECURITY LEVEL (S904)
(6)RECOGNIZE SECURITY LEVEL (S905)
(5)NOTIFY SECURITY LEVEL (S906)
(7)RECOGNIZE SECURITY LEVEL (S907)
(8)SELECT SECURITY LEVEL (S908)
(8)SELECT SECURITY LEVEL (S909)
(A) NOTIFY CERTIFICATE OF USER (S910)
VERIFY NOTIFIED USER CERTIFICATE BY CERTIFICATE OF CERTIFICATION AUTHORITY (S911)
(B) NOTIFY PUBLIC KEY OF SERVER, OR CERTIFICATE OF SERVER (S912)
VERIFY NOTIFIED SERVER CERTIFICATE BY CERTIFICATE OF CERTIFICATION AUTHORITY (S913)
PRODUCE SEED "DEK1" USED FOR VERIFICATION (S914)
(C)NOTIFY PKs(DEK1) PRODUCED BY ENCRYPTING DEK1 BY EMPLOYING PUBLIC ENCRYPTION SYSTEM (S915)
DERIVE DEK1 BY DECODING NOTIFIED PKs(DEK1) BASED ON SECRET KEY OF SERVER (S916)

FIG. 10

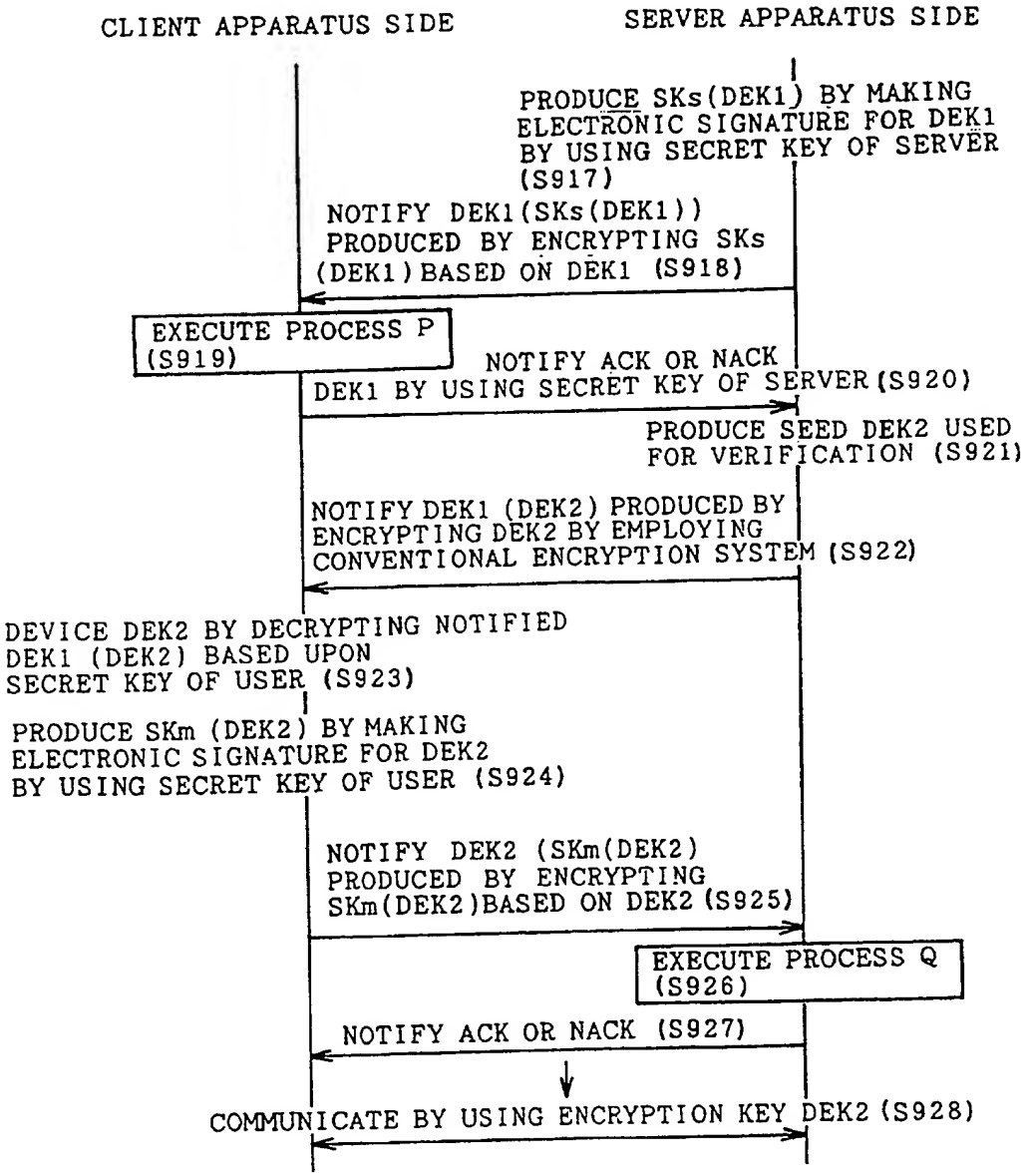

CLIENT APPARATUS SIDE
SERVER APPARATUS SIDE
PRODUCE SKs(DEK1) BY MAKING ELECTRONIC SIGNATURE FOR DEK1 BY USING SECRET KEY OF SERVER (S917)
NOTIFY DEK1(SKs(DEK1)) PRODUCED BY ENCRYPTING SKs (DEK1) BASED ON DEK1 (S918)
EXECUTE PROCESS P (S919)
NOTIFY ACK OR NACK DEK1 BY USING SECRET KEY OF SERVER (S920)
PRODUCE SEED DEK2 USED FOR VERIFICATION (S921)
NOTIFY DEK1 (DEK2) PRODUCED BY ENCRYPTING DEK2 BY EMPLOYING CONVENTIONAL ENCRYPTION SYSTEM (S922)
DEVICE DEK2 BY DECRYPTING NOTIFIED DEK1 (DEK2) BASED UPON SECRET KEY OF USER (S923)
PRODUCE SKm (DEK2) BY MAKING ELECTRONIC SIGNATURE FOR DEK2 BY USING SECRET KEY OF USER (S924)
NOTIFY DEK2 (SKm(DEK2) PRODUCED BY ENCRYPTING SKm(DEK2)BASED ON DEK2 (S925)
EXECUTE PROCESS Q (S926)
NOTIFY ACK OR NACK (S927)
COMMUNICATE BY USING ENCRYPTION KEY DEK2 (S928)

FIG. 11

SECURITY LEVEL "1" (1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(9)

SECURITY LEVEL "2" (1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(B)→(C)→(F)

SECURITY LEVEL "3" (1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(A)→(B)→(C)→(F)→(G)→(H)

SECURITY LEVEL "4" (1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(B)→(C)→(D)→(E)→(F)

SECURITY LEVEL "5" (1)→(2)→(3)→(4)→(5)→(6)→(7)→(8)→(A)→(B)→(C)→(D)→(E)→(F)→(G)→(H)

FIG. 12

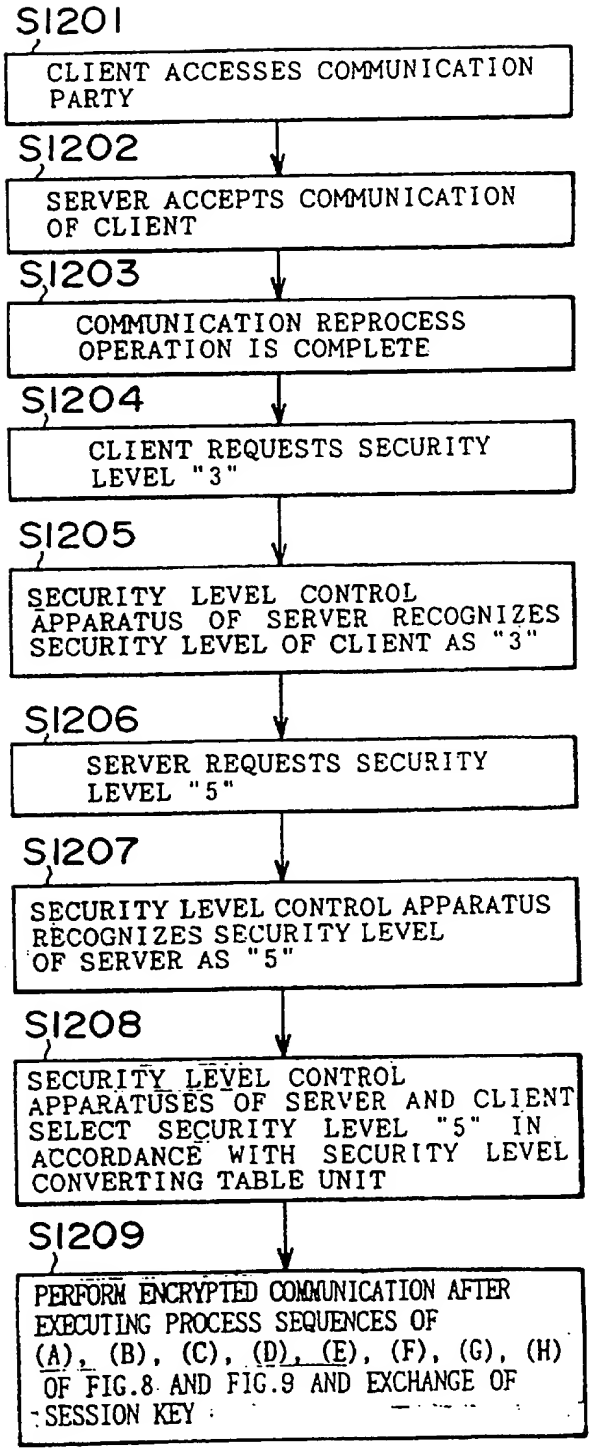
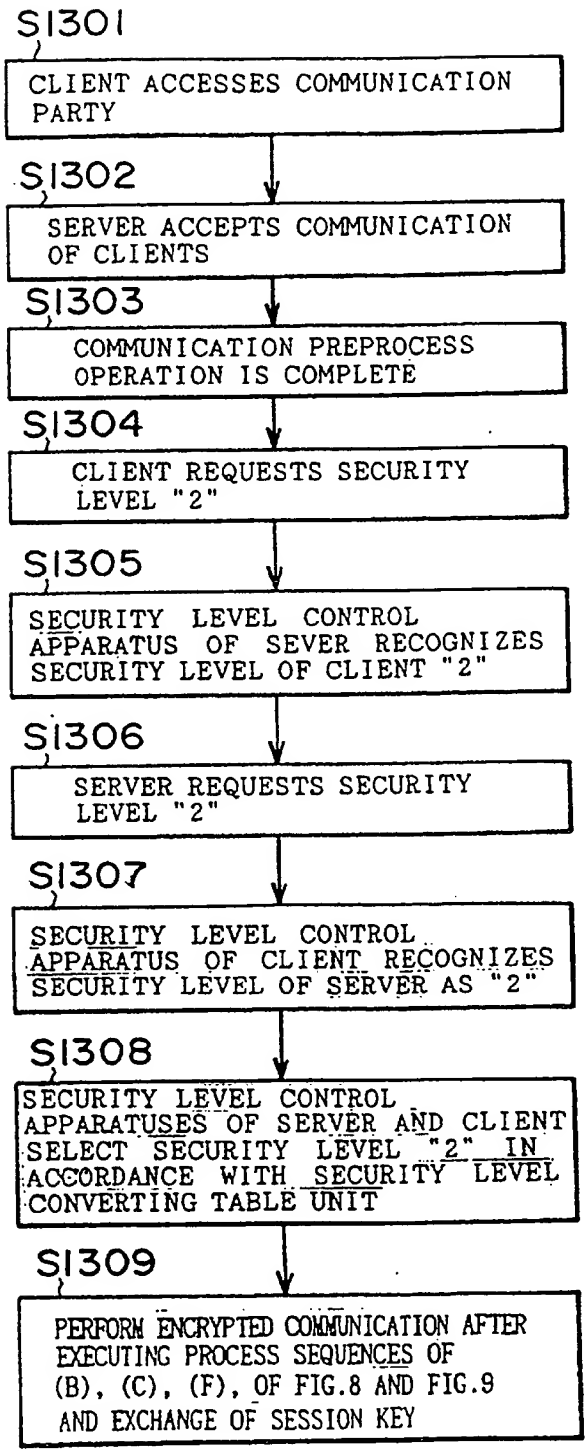

S1201
CLIENT ACCESSES COMMUNICATION PARTY
S1202
SERVER ACCEPTS COMMUNICATION OF CLIENT
S1203
COMMUNICATION REPROCESS OPERATION IS COMPLETE
S1204
CLIENT REQUESTS SECURITY LEVEL "3"
S1205
SECURITY LEVEL CONTROL APPARATUS OF SERVER RECOGNIZES SECURITY LEVEL OF CLIENT AS "3"
S1206
SERVER REQUESTS SECURITY LEVEL "5"
S1207
SECURITY LEVEL CONTROL APPARATUS RECOGNIZES SECURITY LEVEL OF SERVER AS "5"
S1208
SECURITY LEVEL CONTROL APPARATUSES OF SERVER AND CLIENT SELECT SECURITY LEVEL "5" IN ACCORDANCE WITH SECURITY LEVEL CONVERTING TABLE UNIT
S1209
PERFORM ENCRYPTED COMMUNICATION AFTER EXECUTING PROCESS SEQUENCES OF (A), (B), (C), (D), (E), (F), (G), (H) OF FIG.8 AND FIG.9 AND EXCHANGE OF SESSION KEY

FIG. 13



2306865

SECURITY LEVEL CONTROL APPARATUS AND NETWORK COMMUNICATION SYSTEM

The invention relates to a security level control apparatus and to a network communication system.

Network services are commercially available through which electronic mails are provided by mutually connecting computers installed in a distributed manner.

In network systems configured for academic purposes, typically known as the Internet, proper care is not taken to network security matters. Accordingly, these network services are susceptible to security breaches, such as wiretapping, falsification and impersonation.

The term "wiretapping" implies that a plain text, i.e. a correspondence message not yet encrypted is read during message transmission.

The term "falsification" implies that a content of an electronic mail is modified. This falsification is performed in relaying nodes when an electronic mail is delivered via a plurality of relaying nodes.

The term "impersonation" implies that when no protection is established with respect to information for specifying a mail sender, a third party bearing offense falsifies the information for specifying the third party to pose as an impersonator.

To improve security, messages (data) can be encrypted, an electronic signature (Message Integrity Check) can be used to prevent falsification and/or users (communication parties) are subjected to an authentication procedure. In such a network communication system realized in a server/client manner, the server apparatus is authenticated and/or the client apparatus is authenticated.

Encryption techniques such as the secret key cryptosystem, the public key cryptosystem and the like are known. In the secret key cryptosystem, the

encrypting operation and the decrypting operation are carried out by using the common key between the communication parties. In the public key encrypting system, the key system is constituted by combining the secret keys for the individual users with the public keys and the public keys are opened to third parties, whereas the secret keys are disclosed only to the individual users. In this public key cryptosystem, a message which has been encrypted by the public key can be solved by the secret key. For instance, when a message is transmitted from "A" to "B", "A" encrypts this message by using the public key of "B" and then "B", who has received the encrypted message, can decrypt this encrypted message by using the own secret key. The only party who can normally decrypt this encrypted message is "B", since he is normally the only party who knows the secret key.

Authentication techniques such as password authentication and electronic signature with employment of the public key cryptosystem are known.

In the above-described conventional network techniques, a plurality of security levels are produced when certain process operations are combined with each other in order to avoid wiretapping, falsification and impersonation with respect to the network services.

For instance, it is conceivable that a resultant security level becomes high when an electronic mail is encrypted and, at the same time, a user of this electronic mail is authenticated, rather than only the encryption of this electronic mail. When such an idea is made that only the security should be emphasized, it is a better way to combine a large number of processing operations with each other. However, in this case, the resultant workloads would be increased.

Under such a circumstance, it is proper to set the security at a level which reflects the importance of

the communication content concerned. The proper setting of security level based on the importance of a message is called as a "policy of security".

With respect to this "policy of security", drawbacks exist in conventional techniques. Firstly, communication can only be performed between the communication parties in accordance with a predetermined security policy, but cannot be carried out in accordance with other security policies. Secondly, the security level of the communication party (communication destination) is continuously introduced with a top priority, so that ones own security level cannot be reflected.

According to a first aspect of the invention, there is provided a security level control apparatus for controlling a security level of a communication established between communication parties, this security level control apparatus employing a security level recognizing unit and a security level setting unit, wherein the security level recognizing unit recognizes a security level notified from a communication party (for example one of the said communication parties) and wherein the security level setting unit sets the security level recognized by the security level recognizing unit as a security level for the security level control apparatus.

In accordance with an example of the security level control apparatus of the first aspect of the invention, the security level of the communication party recognized by the security level recognizing unit can be first set as the security level for the security level control apparatus. As a result, the communication can be established between the first-mentioned communication parties without presetting the security level.

It can also be designed to execute a communication

while reflecting its own security level.

According to a second aspect of the present invention, there is provided a security level control method for controlling a security level of a communication established between communication parties, comprising step of:

security level recognizing step for recognizing a security level notified from a communication party (for example one of the said communication parties); and

security level setting step for setting the security level recognized by said security level recognizing step.

Other aspects of the invention are exemplified in the attached claims.

For a better understanding of the invention, and to show how the same may be carried into effect, reference will now be made, by way of example, to the accompanying drawings, in which:-

Fig. 1 is a block diagram showing a first security level control apparatus;

Fig. 2 is a block diagram showing a second security level control apparatus;

Fig. 3 is a block diagram showing a first network communication system;

Fig. 4 is a block diagram showing a second network communication system;

Fig. 5 is a block diagram showing a ninth network communication system;

Fig. 6 schematically represents an arrangement of a system according to an embodiment of the present invention;

Fig. 7 is a schematic block diagram for showing an arrangement of the security level control apparatus of the embodiment;

Fig. 8 shows a security level conversion table unit included by the security level control apparatus

of the embodiment;

Fig. 9 schematically represents a first sequential process operation executed between the client apparatus and the server apparatus according to the embodiment;

Fig. 10 schematically represents a second sequential process operation executed between the client apparatus and the server apparatus according to the embodiment;

Fig. 11 schematically indicates a sequential process operation executed in the respective security levels of the embodiment;

Fig. 12 is a flow chart for indicating a first process operation according to the embodiment; and

Fig. 13 is a flow chart for indicating a second process operation according to the embodiment.

FIRST SECURITY LEVEL CONTROL APPARATUS 10

Figure 1 shows a security level control apparatus 10 for controlling a security level of a communication executed between communication parties, the apparatus comprising a security level recognizing unit 11 and a security level setting unit 14.

The security level recognizing apparatus 11 recognizes a security level notified from a communication destination (a communication party).

The security level setting unit 14 sets the security level recognized by the security level recognizing unit 11 as a security level for the security level control apparatus 10.

The security level of the communication party recognized by the security level, in turn recognized by the security level recognizing unit 11, is set as the security level for security level control apparatus 10.

SECOND SECURITY LEVEL CONTROL APPARATUS 10

Figure 2 shows a security level control apparatus 10 for controlling the security level of communication between communication parties, the apparatus comprising

a security level recognizing unit 11, a security level converting table unit 12, a security level reading unit 13 and a security level setting unit 14.

The security level recognizing apparatus 11 recognizes a security level notified from communication destination (communication party).

The security level converting table unit 12 stores a relationship between an index made of two sets of security levels, and a security level of an actual communication.

The security level reading unit 13 reads from the security level converting table unit 12, a security level corresponding to such an index. This index is defined by the security level of the communication party recognized by the security level recognizing unit 11 and the security level for the security level control apparatus 10.

The security level setting unit 14 sets the security level recognized by the security level recognizing unit 11 as the security level for the security level control apparatus 10.

Both the security level of the communication party recognized by security level recognizing unit 11 and the security level for security level control apparatus 10 are set as the index. Then, the security level corresponding to this index is read from the security level converting table unit 12. Thus, this read security level is set as the security level for the security level apparatus 10.

FIRST NETWORK COMMUNICATION SYSTEM

Figure 3 shows a network communication system provided with a server apparatus 20 and a client apparatus 30, which perform a communication whose security level is set, the client apparatus 30 includes a security level control apparatus 10. This security level control apparatus 10 is constructed of a security

level recognizing unit 11 and a security level setting unit 14.

The security level recognizing unit 11 recognizes a security level notified from a communication party (communication destination).

The security level setting unit 14 sets the security level recognized by the security level recognizing unit 11 as a security level for the client apparatus 30.

On the side of the client apparatus 30, the security level of the server apparatus 20 recognized by the security level recognizing unit 11 is set as the security level for the client apparatus 30.

SECOND NETWORK COMMUNICATION SYSTEM

Figure 4 shows a network communication system provided with a server apparatus 20 and a client apparatus 30, which perform a communication whose security level is 25 set, the server apparatus 20 includes a security level control apparatus 10. This security level control apparatus 10 is constructed of a security level recognizing unit 11 and a security level setting unit 14.

The security level recognizing unit 11 recognizes a security level notified from a communication party (communication destination).

The security level setting unit 14 sets the security level recognized by the security level recognizing unit 11 as a security level for the server apparatus 20.

On the side of the server apparatus 20, the security level of the client apparatus 30 recognized by the security level recognizing unit 11 is set as the security level for the server apparatus 20.

THIRD NETWORK COMMUNICATION SYSTEM

A third network communication system (not shown) comprises a plurality of server apparatuses 20.

The security level control apparatus 10 provided with the client apparatus 30 controls the security level with respect to each of the server apparatuses 20. The security levels are controlled every server apparatus 20.

FOURTH NETWORK COMMUNICATION SYSTEM

A fourth network communication system (not shown) comprises a plurality of the above-described client apparatuses 30. The security level control apparatus 10 employed in the server apparatus 20 controls the security levels with respect to each of the client apparatuses 30.

The security level is controlled with respect to each of the client apparatuses 30.

FIFTH NETWORK COMMUNICATION SYSTEM

A fifth network communication system (not shown) is a modification of either the first or the third network communication system, in which the security level control apparatus 10 of the client apparatus 30 includes a security level converting table unit 12 and a security level reading unit 13.

The security level converting table unit 12 stores a relationship between an index constructed of two sets of security levels and an actual communication security level.

The security level reading unit 13 reads from the security level converting table unit 12, a security level corresponding to such an index that is constructed of a security level of a communication party recognized by the security level recognizing unit 11 and the security level for the client apparatus 30.

The security level setting unit 14 sets the security level read from the security level reading unit 13 as the security level for the client apparatus 30.

In operation, the security level of the server

apparatus 20 recognized by the security level recognizing unit 11 and the security level for the client apparatus 30 are used as the index. The security level corresponding to this index is read from the security level converting table unit 12. This read security level is set as a security level for the client apparatus 30.

SIXTH NETWORK COMMUNICATION SYSTEM

A sixth network communication system is a modification of either the second or the fourth network communication system, in which the security level control apparatus 10 of the server apparatus 20 includes a security level converting table unit 12 and a security level reading unit 13.

The security level converting table unit 12 stores a relationship between an index constructed of two sets of security levels and an actual communication security level.

The security level reading unit 13 reads from the security level converting table unit 12, a security level corresponding to such an index that is constructed of a security level of the client apparatus recognized by the security level recognizing unit 11 and the security level for the server apparatus 20.

The security level setting unit 14 sets the security level read from the security level reading unit 13 as the security level for the server apparatus 20.

In operation, the security level of the client apparatus 30 recognized by the security level recognizing unit 11 and the security level for the server apparatus 20 are used as the index. The security level corresponding to this index is read from the security level converting table unit 12. This read security level is set as a security level for the server apparatus 20.

SEVENTH NETWORK COMMUNICATION SYSTEM

A seventh network communication system (not shown) comprises a security level control apparatus 10 of the client apparatus 30 capable of dynamically changing the security level, even during the communication, in response to a request from the client apparatus 30.

EIGHTH NETWORK COMMUNICATION SYSTEM

An eighth network communication system (not shown) comprises a security level control apparatus of the server apparatus capable of dynamically changing the security level, even during the communication, in response to a request from the server apparatus.

NINTH NETWORK COMMUNICATION SYSTEM

Figure 5 shows a network communication system provided with a server apparatus 20 and a client apparatus 30, which perform a communication whose security level is set. The server apparatus 20 and the client apparatus 30 include security level control apparatuses 10. This security level control apparatus 10 is constructed of a security level recognizing unit 11, a security level converting table unit 12, a security level reading unit 13 and a security level setting unit 14.

The security level recognizing unit 11 recognizes a security level notified from a communication party.

The security level converting table unit 12 stores a relationship between an index constructed of two sets of security levels and an actual communication security level.

The security level reading unit 13 reads from the security level converting table unit 12, a security level corresponding to such an index that is constructed of the security level of the communication party recognized by the security level recognizing unit 11 and 5 the security level for the security level control apparatus 10.

The security level setting unit 14 sets the security level read from the security level reading unit 13 as the security level for the security level control apparatus 10.

In operation, both the security level of the communication party recognized by the security level recognizing unit 11 and the security level for the security level control apparatus 10 are used as the index. The security level corresponding to this index is read from the security level converting table unit 12. This read security level is set as the security level for the security level apparatus 10.

TENTH NETWORK COMMUNICATION SYSTEM

A tenth network communication system (not shown) comprises a security level control apparatus 10 of the client apparatus 30 capable of dynamically changing the security level, even during the communication, in response to a request from the client apparatus 30. The security level control apparatus 10 of the server apparatus 20 is also capable of dynamically changing the security level, even during the communication, in response to a request from the server apparatus 20.

Various embodiments of the present invention will now be described with reference to the drawings.

A system of an embodiment is arranged by employing a server apparatus 20 (also, referred to as a "server"), as shown in Fig. 6, a network 40 connected to this server apparatus, and a client apparatus 30 (also, referred to as a "client") connected to this network 40.

In this system, a communication is established between the server apparatus 20 and the client apparatus 30. To prevent wiretapping, falsification, and impersonator in the communication, five stages of security levels can be set in accordance with the importance of communication contents.

It should be noted that although only one server apparatus 20 is indicated in Fig. 6, a plurality of server apparatuses may be employed. Similarly, although only one client apparatus 30 is shown in this drawing, a plurality of client apparatuses may be employed.

(SECURITY LEVEL)

When the communication starts, the server apparatus 20 and the client apparatus 30 notify to each other their respective independently set security levels. Therefore, the server apparatus 20 and the client apparatus 30 communicate in accordance with security levels determined based upon the mutual security levels.

As mentioned above the security levels may be set in five stages. These five-staged security levels are set as follows:

Security Level "1"---	Neither encryption nor authentication is performed (so-called normal communication).
Security Level "2"---	Only encryption is carried out.
Security Level "3"---	Both encryption and user authentication are performed.
Security Level "4"---	Both encryption and server authentication are carried out - n.b. security level "4" is a security level equivalent to security level "3".
Security Level "5"---	Encryption, user authentication and server authentication

are carried out.

When a plurality of client apparatuses 30 are provided, the server apparatus 20 may communicate in response to the security levels independently set for the respective client apparatuses 30.

When a plurality of server apparatuses 20 are provided, the client apparatus 30 may communicate in response to the security levels independently set for the respective server apparatuses 20.

Then, as the security level, other items may be set as follows. That is, no encryption is carried out at the security levels "2" to "5", and alternatively, the client is authenticated at the security levels "2" to "5".

Furthermore, the expression "user authentication" involves authentication by password and authentication by a public key certification. This embodiment describes the authentication by public key certification.

(ARRANGEMENT OF SERVER APPARATUS 20)

The server apparatus 20 is arranged by employing a communication control unit 21 connected to the network 40, a service processing unit 22 connected to this communication control unit 21, a security level control apparatus 10 connected to this service processing unit 22 and a storage unit 23 connected to the service processing unit 22.

The communication control unit 21 controls the communication established between the server apparatus 20 and the network 40.

To accept various service requests issued from the server apparatus 20, the service processing unit 22 transmits/receives the data among the security level control apparatus 10, the communication control unit 21 and the storage unit 23.

The storage unit 23 stores therein information

concerning a user secret key (SKm: "m" being subscript), a user certification (CERTm: "m" being subscript), and a certification of an issuing station (CERTca: "ca" being subscript). As this storage unit 23, a RAM (Random Access Memory), a semiconductor memory device, a magnetic disk storage apparatus, a magnetic tape recording apparatus, an M/O (Magneto-Optical) disk apparatus or an IC card etc may be employed.

The security level control apparatus 10 is an apparatus for controlling security of actually performed communications based upon the security level notified from the client apparatus 30 and the security level owns by the server apparatus 20 when the communication is commenced. An arrangement of the security level control apparatus 10 will be explained subsequent to the description about the arrangement of the client apparatus 30.

(ARRANGEMENT OF CLIENT APPARATUS 30)

The client apparatus 30 is arranged by employing a communication control unit 31 connected to the network 40, a service processing unit 32 connected to this communication control unit 31, a security level control apparatus 10 connected to this service processing unit 32 and a storage unit 33 connected to the service processing unit 32.

The communication control unit 31 controls the communication established between the server apparatus 20 and the network 40.

To accept various service requests issued from the client apparatus 30, the service processing unit 32 transmits/receives the data among the security level control apparatus 10, the communication control unit 31 and the storage unit 33.

The storage unit 33 stores therein information concerning a server Public key (PKs: "s" being

subscript), a server certificate (CERTs: "s" being subscript), a server secret key (SKs: "s" being subscript) and a certificate of an Certification Authority (CERTca: "ca" being subscript). As this storage unit 33 a RAM (Random Access Memory), a semiconductor memory device, a magnetic disk storage apparatus, a magnetic tape recording apparatus, an M/O (Magneto-Optical) disk apparatus or an IC card etc. may be employed.

The security level control apparatus 10 is an apparatus for negotiating the security level notified from the server apparatus 20 with the security level of the client apparatus 30 when the communication is commenced.

(ARRANGEMENT OF SECURITY LEVEL CONTROL APPARATUS 10)

Since the security level control apparatus 10 provided with the server apparatus 20 is arranged similar to the security level control apparatus 10 employed in the client apparatus 30, the arrangement thereof will now be described without giving any discrimination.

As shown in Fig. 7, the security level control apparatus 10 is constituted by employing a control unit 16, a security level recognizing unit 11, a security level converting table unit 12, a security level setting unit 14, a security level notifying unit 15, an encryption processing unit 17, and an authentication processing unit 18.

The control unit 16 is connected to either the service processing unit 22 (in case of server apparatus 20) or the service processing unit 32 (in case of client apparatus 30), and also connected to the security level recognizing unit 11, the security level converting table unit 12, the security level reading unit 13, the security level setting unit 14, the security level notifying unit 15, the encryption

processing unit 17, and the authentication processing unit 18. Then, the control unit 16 controls data transmitting/receiving operations among these units.

The security level recognizing unit 11 recognizes the security level notified from the communication party.

The security level converting table unit 12 sets the index of the server to 1 through 5, and also the index of the client to 1 through 5 in such a case that the security levels used in the network are set to five stages, i.e., 1 through 5, which all the servers and all the clients can own in order that any of these servers and clients can use this converting table. Then, the security level converting table unit 12 is arranged in such a manner that any one of the 25 patterns in total can be obtained based upon the security levels requested by the respective servers and clients which actually perform the communications.

In Fig. 8, there is shown the security level converting table unit 12 according to this embodiment. In the case of Fig. 8, assuming now that the security level of the client is "2" and the security level of the server is "4", the security level of the actual communication becomes "4". It should be noted in this drawing that a portion indicated as "X" implies that no communication can be performed at the security levels set by the server apparatus 20 and the client apparatus 30. In other words, this "X" portion corresponds to such a case that the security levels cannot be controlled.

As described above, the security level converting table unit 12 according to this embodiment is arranged as the following table, considering that the information provided by the server is important. That is, when the security level requested by the server is higher than the security level requested by the client,

the security level requested by the server may have a priority.

However, the structure of the security level converting table unit 12 is not limited to the above described embodiment. Alternatively, for example, the security level converting table unit 12 may be arranged by that only a security level which can be required by an own apparatus is set as a first index, and all of security levels which can be required by a counter party's apparatus are set as a second index. For instance, assuming now that in the above-described network, the own apparatus corresponds to the client which can require the security levels 1 through 3, and that the counter party's apparatus corresponds to the server which can require the security levels 1 through 5, any one of 15 patterns may be obtained, namely 15 patterns (in total) = indexes (3) of own apparatus x indexes (5) of the server.

While using the security level of the communication party recognized by the security level recognizing unit 11 and the security level for the security level control apparatus 10, as the index, the security level reading unit 13 reads a security level corresponding to this index from the security level converting table unit 12.

The security level setting unit 14 sets the security level read out from the security level reading unit 13 as the security level for the security level control apparatus 10.

The security level notifying unit 15 notifies the own security level to the communication party.

The encryption processing unit 17 encrypts a message to be outputted to the communication party, and conversely, decrypts the encrypted message entered from the communication party. It should be understood in this embodiment that the DES (Data Encryption Standard)

system is utilized as the secret key cryptosystem, whereas the RAS (Rivest-Shamir-Aldeman) system is employed as the public key cryptosystem.

The authentication processing unit 18 performs server authentication (in case of client apparatus 30), and user authentication.

(SEQUENTIAL PROCESS OPERATION BETWEEN CLIENT APPARATUS 30 AND SERVER APPARATUS 20)

Referring now to Fig. 9 and Fig. 10, a description will be made of sequential process operation between the client apparatus 30 and the server apparatus 20 in the embodiment mode. It should be understood that all of the sequential process operations are not executed in this explanation, but only necessary process operations are executed every security level.

First, the client apparatus 30 notifies a communication request to the server apparatus 20 (step 901, this notification is expressed as "1"). In response this communication request, the server apparatus 20 notifies acceptance to the client apparatus 30 (step 902, this notification is indicated as "2").

After the acceptance is notified to the client apparatus 30, a communication pre-process operation is carried out between the client apparatus 30 and the server apparatus 20 (step 903, this pre-process operation is indicated by "3"). In this case, the communication pre-process operation implies information exchanges, for instance, information about terminal type, information about display system (how information is displayed by which line, which digit), information about sort of used character code, and IP address.

After the pre-process operation is complete, the client apparatus 30 notifies the security level set by the client apparatus 30 to the server apparatus 20 (step) 904, this notification is indicated by "4").

Upon receipt of this notification, the server apparatus 20 recognizes the security level set by the client apparatus 30 (step 905, this recognition is indicated by "6").

Subsequently, the sever apparatus 20 notifies the security level set by the server apparatus 20 to the client apparatus 30 (step 906, this notification is indicated by "5"). Upon receipt of this notification, the client apparatus 30 recognizes the security level set by the server apparatus 20 (step 907, this recognition is denoted by "7").

In accordance with the security level set by the client apparatus 30 and the security level notified from the server apparatus 20, the client apparatus 30 selects the security level of the actually performed communication (step 908, this selection is expressed by "8").

In accordance with the security level set by the server apparatus 20 and the security level notified from the client apparatus 30, the server apparatus 20 selects the security level of the actually performed communication (step 909, this selection is expressed by "8").

It should be understood that the security levels selected at the step 908 and the step 909 are coincident with each other.

Thereafter, the client apparatus 30 notifies the user certification (CERTm) to the server apparatus 20 (step 910, this notification is expressed by "A").

The server apparatus 20 verifies the notified user certificate based on the certificate of the Certification Authority (CERTca) (step 911).

The server apparatus 20 notifies the public key (PKs) of the server, or the certification (CERTs) of the server to the client apparatus 30 (step 912, this notification is indicated by "B").

The client apparatus 30 verifies the notified certificate (CERTs) of the server based upon the certificate (CERTca) of the issuing Certification Authority (step 913).

Also, the client apparatus 30 produces "DEK1" corresponding to seed for authentication (in this case, authentication of server) by way of random numbers (step 914)

Thereafter, the client apparatus 30 notifies to the server apparatus 20, PKs (DEK1) produced by encrypting "DEK1" based upon the public key (PKs) of the server (step 915, this notification is indicated by "C"). In other words, the client apparatus 30 corresponding to a "sender" encrypts a session key used to read the statement based on the public key (PKs) of the server apparatus 20 corresponding to a "receiver". Up to the present processing stage, since there is no session key for the client apparatus 30 and the server apparatus 20, the encryption is carried out by way of the public key cryptosystem (RSA).

The server apparatus 20 derives DEK1 by decoding the notified PKs (DEK1) by the secret key (SKs) of the server (step 916). In other words, the server apparatus 20 functioning as the receiver decodes the session key by using the secret key (SKs) of the server corresponding to the own secret key. Thereafter, the content sent from the client apparatus 30 is decoded by the decoded session key.

The server apparatus 20 produces SKs(DEK1) by performing DEK1 with employment of the server secret key (SKS) (step 917).

Thereafter, the server apparatus 20 notifies DEK1(SKs(DEK1)) produced by encrypting SKS(DEK1) by DEK1 to the client apparatus 30 (step 918, this notification is indicated by "D"). In this case, the reason why SKS(DEK1) is encrypted by DEK1 is that an

electronic signature is not wiretapped. The reason why such an electronic signature is made is to investigate that the sender (user) is authenticated and the content of the statement is not falsified. For example, a signer "A" makes up a digest of the statement by using a proper hash function, and then encrypts this digest by employment of a secret key for this signer "A". This may constitute a signature. A verifier "B" verifies the signature by employing the public key of the signer "A" to be returned to the original signature so as to check whether or not this result is equal to the digest of the original statement. If this result is not equal to the digest of the original statement, then it can be seen that the statement is falsified.

Now, the client apparatus 30 executes the following items 1) to 3) as a process "P" (step 919).
1). DEK1(SKs(DEK1)) is decoded to derive SKs(DEK1).
2). DEK1 is derived from the derived SKs(DEK1) by employing the public key (PKs) contained in the certificate of the server. 3). The derived DEK1 is compared with DEK1 produced at the step 914. With this comparison, the server is authenticated. The reason why this authentication is perform is to confirm as to whether or not the public key opened as the server certificate is really the key for the server apparatus 20. This confirmation is performed by employing the server certificate (CERTs) authenticated by a third party. Such a confirmation is also called as "third party authentication", or "electronic notary public". Simply speaking, a counter party makes a signature on a mail sent by an owner, and if this signature decrypted by employing the public key of the third party is identical to the signature sent by the owner, then the authentication can be established.

As a comparison result of the item 3) at the step 919, if the received signature is identical to the

original signature, then the client apparatus 30 notifies "ACK" to the server apparatus 20, whereas if the received signature is not identical to the original signature, then the client apparatus 30 notifies "NACK" to the server apparatus 20.

Next, the server apparatus 20 produces DEK2 corresponding to a seed for authentication (in this ease, authentication of user) by using random numbers (step 921).

Subsequently, the server apparatus 20 notifies to the client apparatus 30, DEK1(DEK2) produced by encrypting DEK2 by utilizing the secret key cryptosystem (step 922, this notification is indicated by "F"). In this ease, the reason why the secret key cryptosystem is employed is such that the encryption key DEK1 is commonly used in the client apparatus 30 and the server) apparatus 20, and when this encryption key DEK1 is utilized, the processing speed can be increased. In other words, if all of process of encryption is done by Public key Cryptosystem.

Subsequently, the client apparatus 30 derives DEK2 by decoding the DEK1(DEK2) notified from the server apparatus 20 by way of the secret key (SKm) of the user (step 923).

Also, the client apparatus 30 produces SKm(DEK2) by making an electronic signature with respect to DEK2 by) employing the secret key (SKm) of the user (step 924).

Thereafter, the client apparatus 30 notifies DEK2(SKm(DEK2)) produced by encrypting SKm(DEK2) by using DEK2 (step 925, this notification is expressed by "G").

Now, the server apparatus 20 executes the following items 1) to 3) as a process "Q" (step 926). 1). DEK2(SKm(DEK2)) is decoded to derive SKm(DEK2). 2). DEK2 is derived from the derived SKm(DEK2) by employing

the user secret key (SKm). 3). The derived DEK2 is compared with DEK2 produced at the step 921. With this comparison, the user is authenticated.

As a comparison result of the item 3) at the step 926, if the decrypted signature is identical to the original signature, then the server apparatus 20 notifies "ACK" to the client apparatus 30, whereas if the received signature is not identical to the original signature, then the server apparatus 20 notifies "NACK" to the client apparatus 30 (step 927, this notification is repressed by "H").

Thereafter, a communication is carried out by employing the-session key DEK2 between the client apparatus 30 and the server apparatus 20 (step 928, this communication is indicated by "9").

(SEQUENTIAL PROCESS OPERATIONS EXECUTED IN RESPECTIVE SECURITY LEVELS)

The sequential process operations executed in the respective security levels will now be explained with reference to Fig. 11.

First, in the security level "1", the above explained process operations (1), (2), (3), (4), (5), (6), (7), (8) and (9) are carried out in this order.

Next, in the security level "2", the above-described process operations (1), (2), (3), (4), (5), (6), (7), (8), (B), (C) and (F) are performed in this order.

Then, in the security level "3", the above described process operations (1), (2), (3), (4), (5), (6), (7), (8), (A), (B), (C), (F), (G) and (H) are sequentially executed.

Then, in the security level "4", the above described process operations (1), (2), (3), (4), (5), (6), (7), (8), (B), (C), (D), (E) and (F) are sequentially executed.

Next, in the security level "5", the above

described process operations (1), (2), (3), (4), (5), (6), (7), (8), (B), (C) and (D), (E), (F), (G) and (H) are performed in this order.

(FIRST PROCESS OPERATION)

Referring now to Fig. 12, the first process operation will be explained;

First, the client apparatus 30 (client) accesses a communication party (step 1201).

Next, the server apparatus 20 (server) accepts the communication by the client (step 1202).

At this stage, the communication pre-process operation is complete (step 1203).

Thereafter, the client requests the security level "3" (step 1204).

In response to this request, the security level control apparatus 10 of the server recognizes that the security level of the client is equal to "3" (step 1205).

Next, the server requests the security level "5" (step 1206).

In response to this request, the security level control apparatus 10 of the client recognizes that the security level of the server is equal to "5" (step 1207).

At this stage, the security level control apparatuses 10 of the server and the client select the security level "5" in accordance with the security level converting table unit 12 (step 1208).

Both the server and the client perform the encryption communication after executing the sequential process operations (A), (B), (C), (D), (E), (F), (G) and (H) of Fig. 9 and Fig. 10, and also exchange of the session keys (step 1209).

(SECOND PROCESS OPERATION)

Referring now to Fig. 13, the second process operation will be explained.

First the client apparatus 30 (client) accesses a communication party (step 1301).

Next, the server apparatus 20 (server) accepts the communication by the client (step 1302).

At this stage, the communication pre-process operation is complete (step 1303).

Thereafter, the client requests the security level "2" (step 1304).

In response to this request, the security level control apparatus 10 of the server recognizes that the security level of the client is equal to "2" (step 1305).

Next, the server requests the security level "2" (step 1306).

In response to this request, the security level control apparatus 10 of the client recognizes that the security level of the server is equal to "2" (step 1307).

At this stage, the security level control apparatuses 10 of the server and the client select the security level "2" in accordance with the security level converting table unit 12 (step 1308).

Both the server and the client perform the encryption communication after executing the sequential process operations (B), (C), and (F) of Fig. 9 and Fig. 10, and also exchange of the session keys (step 1309).

As previously described in detail, the communication level is not determined based upon only the communication level requested by the counter party's apparatus, but the actual communication level is determined based on the communication levels requested by both parties' apparatuses in this embodiment. As a consequence, the following effects can be achieved. That is, in the case that this embodiment is applied to the Internet, when a communication is established between a server and a

user apparatus (called as a "host" in the Internet field), the security level converting table unit 12 is arranged in such a manner that the level requested by the server owns a priority so as to avoid the problems even under such a condition that although the server wants to encrypt the information in order to avoid that other apparatuses may refer to this information, the user requests to communicate the "plain text".

Furthermore, if the respective roles of the server and client are interchanged, certain of the above-mentioned effects of preferred embodiments of the invention can still be achieved.

CLAIMS:

1. A security level control apparatus for controlling the security level of communication established between communication parties, the apparatus comprising:

security level recognizing means for recognizing a security level notified from one of the communication parties; and

security level setting means for setting the security level of the security level control apparatus to the security level recognized by the security level recognizing means.

2. A security level control apparatus for controlling the security level of communication established between communication parties, the apparatus comprising:

security level recognizing means for recognizing a security level notified from one of the communication parties;

security level converting table means for storing therein a relationship between an index having two sets of security levels and a security level of an actual communication;

security level reading means for setting the security level of the communication party recognized by said security level recognizing means and a security level of said security level control apparatus as said index, and for reading a security level corresponding to said index from said security level converting table means; and

security level setting means for setting the security level of the security level control apparatus to the security level read from the security level reading means.

3. A server apparatus for use in a system wherein said communication parties include at least one

client apparatus and at least one server apparatus, said server apparatus comprising a security level control apparatus according to claim 1 or 2.

4. A client apparatus for use in a system wherein said communication parties include at least one client apparatus and at least one server apparatus, said client apparatus comprising a security level control apparatus according to claim 1 or 2.

5. A network communication system comprising a server apparatus and a client apparatus, said client apparatus comprising a security level control apparatus for controlling the security level of communication established between the client apparatus and the server apparatus,

said security level control apparatus comprising:

security level recognizing means for recognizing a security level notified from a communication party; and

security level setting means for setting the security level of said client apparatus to the security level recognized by said security level recognizing means.

6. A network communication system comprising a server apparatus and a client apparatus, said server apparatus comprising a security level control apparatus for controlling the security level of communication established between the client apparatus and the server apparatus,

said security level control apparatus comprising:

security level recognizing means for recognizing a security level notified from a communication party; and

security level setting means for setting the security level of said server apparatus to the security level recognized by said security level recognizing means.

7. A network communication system as claimed in claim 5 comprising a plurality of server apparatuses,

said security level control apparatus comprising means for controlling the security level with respect to each of said server apparatuses.

8. A network communication system as claimed in claim 6 comprising a plurality of client apparatuses, said security level control apparatus comprising means for controlling the security level with respect to each of said client apparatuses.

9. A network communication system as claimed in claim 5 or claim 7 wherein the security level control apparatus comprises:

security level converting table means for storing therein a relationship between an index constituted by two sets of security levels and a security level of an actual communication; and

security level reading means for setting the security level of said server apparatus recognized by said security level recognizing means and a security level of said client apparatus as said index, and for reading a security level corresponding to said index from said security level converting table means; and

said security level setting means sets the security level read out from said security level reading means as a security level for said client apparatus.

10. A network communication system as claimed in claim 6 or claim 8 wherein the security level control apparatus comprises:

security level converting table means for storing therein a relationship between an index constituted by two sets of security levels and a security level of an actual communication; and

security level reading means for setting the security level of said client apparatus recognized by said security level recognizing means and a security level of said server apparatus as said index, and for

reading a security level corresponding to said index from said security level converting table means; and

said security level setting means sets the security level read out from said security level reading means as a security level for said server apparatus.

11. A network communication system as claimed in claim 9 wherein the security level control apparatus has means for dynamically changing the security level in response to a request of said client apparatus, even during executions of the communication.

12. A network communication system as claimed in claim 10 wherein the security level control apparatus has means for dynamically changing the security level in response to a request of said server apparatus, even during executions of the communication.

13. A network communication system comprising a server apparatus according to claim 3 and a client apparatus according to claim 4.

14. A network communication system as claimed in claim 13 wherein:

the security level control apparatus of the client apparatus has means for dynamically changing the security level in response to a request of the client apparatus, even during executions of the communication; and

the security Level control apparatus of the server apparatus has means for dynamically changing the security level in response to a request of the server apparatus, even during executions of the communication.

15. A method for controlling the security level of communication established between communication parties, the method comprising recognizing a security level notified from one of the communication parties and setting the security level for the communication to the recognized security level.

16. A method for controlling the security level of communication established between communication parties, the method comprising:

a security level recognizing step for recognizing a security level notified from one of the communication parties;

a security level converting step for storing therein a relationship between an index having two sets of security levels and a security level of an actual communication;

a security level reading step for setting the security level of the communication party recognized by said security level recognizing step and a security level obtained by said security level converting step as said index, and for obtaining a security level corresponding to said index from said security level converting step; and

a security level setting step for setting the security level obtained from said security level reading step.

17. A security level control apparatus substantially as hereinbefore described with reference to the accompanying drawings.

18. A client or server apparatus substantially as hereinbefore described with reference to the accompanying drawings.

19. A network communication system substantially as hereinbefore described with reference to the accompanying drawings.

20. A method for controlling the security level of communication between parties substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

32

Application No: GB 9621161.0
Claims searched: 1-20

Examiner: Ken Long
Date of search: 20 January 1997

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): H4P (PDCSA & PDCSX)

Int Cl (Ed.6): H04L (9/32 & 9/00)

Other: ONLINE : WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 0534679 A2	AT & T (page 2 lines 3-5 & 38-42 and Table 2 page 6)	1 and 15
X	EP 0520709 A2	DEC (column 1 lines 53-58, column 5 lines 41-56, column 10 lines 17-25 and column 11 lines 51-55)	1-3, 6, 7, 9, 15 and 16
X	EP 0409397 A2	ICL (column 1 line 52 to column 2 line 7 and column 4 lines 20 - 43)	1-10, 13, 15 and 16
X	EP 0375139 A2	IBM (column 2 lines 3-22 & 48-55)	1 and 15
X	EP 0375138 A2	IBM (column 2 lines 13-35)	1 and 15
X	US 5369707	TECSEC (column 4 lines 43-48 &63-68 and column 5 lines 46-51)	1 and 15

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.